ATTACHMENT 10

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

SURGICAL INSTRUMENT SERVICE COMPANY, INC., Plaintiffs, v. INTUITIVE SURGICAL, INC., Defendants.	Case No. 3:21-cv-03496-VC Honorable Vince Chhabria

EXPERT REPORT OF PAUL D. MARTIN, PH.D.

January 18, 2023

Highly Confidential – Subject to Protective Order

1. My name is Paul D. Martin, Ph.D. I have been retained as an expert on behalf of Defendant Intuitive Surgical, Inc., in the above captioned matter. I have been asked to submit this report covering certain technical matters at issue in the case.

I. QUALIFICATIONS

2. I am presently the Director of Firmware Security and Senior Research Scientist for Harbor Labs, Inc. I hold B.S., M.S.E., and Ph.D. degrees from Johns Hopkins University, with all degrees, including my doctorate, being in computer science. My current curriculum vitae (CV) is attached to this report as Attachment A. My education and experience in these fields are set forth in detail there. Attachment A also includes a list of publications authored in the previous 10 years and a list of all other cases in which I have testified or been deposed in the past four years.
3. I am an expert in the technical subject matter areas relevant to this report. All opinions and facts stated in this report are true and correct to the best of my knowledge. If called upon to testify, I could and would testify to the truth of the following.
4. Harbor Labs is being compensated for my time at an hourly rate of $580 per hour. My compensation and the compensation to Harbor Labs is not dependent on and has not affected the substance of my statements in this report. Neither my compensation nor that of Harbor Labs is affected by or contingent upon the ultimate outcome of this litigation, and I have no other interest in this proceeding.
5. I first started programming at the age of 14 with the C programming language. I began writing source code in C, Python, and Java shortly thereafter. I began working in the software industry in 2008, when I obtained my first independent consulting client—the

Brandeis University Hardware Repair Shop. I wrote and edited the source code to a program for their ticketing system to interface with a label printer. This enabled the computer repair shop to automatically print labels associated with tickets in order to easily identify customers' devices.

6. In 2009, I began working for a security consulting company called Independent Security Evaluators in Baltimore, Maryland. I worked on a wide variety of security and privacy projects including projects to test and break the DRM scheme of a magazine distribution application for IOS and Android (at the behest of the developer of said application), projects to test implementation code for cryptographic secret splitting, projects to assist with fuzz testing for security vulnerabilities of a variety of software applications, software development projects to automate testing of antivirus and antimalware solutions, and a variety of other security-related projects. I worked for ISE as an intern throughout the semesters and summers until August 2011. In 2010, I also designed a security architecture for a large-scale digital curation system meant to be a major inter-university initiative to create a successor to existing digital curation systems that could be used for decades.

7. In spring 2011, I completed my bachelor's in computer science at Johns Hopkins University, and I also retained an independent consulting client, the University of Michigan, for whom I performed a penetration test and security assessment of a cloud-based research system that they planned to deploy. In fall 2011, I began working towards my Ph.D. in computer science, also at Johns Hopkins University, and I began researching computer security and privacy systems in order to both design novel technologies for securing computing systems and to also bridge the interface gap between users and their technology. As such, my research focused not only on developing technical solutions to

novel security and privacy systems but also on presenting these solutions in a way that non-technical users could understand.

8. During my time as a Ph.D. student at Johns Hopkins, I co-instructed a short course called, "Introduction to Hardware Hacking," with a colleague, Dr. Michael Rushanan, which was the highest-rated course in the computer science department (based on student reviews) during the winter session in which it was offered. In this course, we offered lessons on a variety of topics including modifying game consoles and device firmware; electronics repair; binary analysis and modification; network traffic analysis; and web-based vulnerability assessment and exploitation.

9. I finished my Ph.D. by successfully defending my dissertation, entitled "Securing Medical Devices and Protecting Patient Privacy in the Technological Age of Healthcare," on February 12, 2016, at the age of 26. My doctoral thesis tells the story of a secure healthcare practice of the future in which technology is seamless to use for healthcare providers while providing a much higher standard of security than is typical today. It focuses on the juxtaposition of usability and security with an emphasis on simplicity, automation, and error-proofing of security controls.

10. During my doctorate and afterwards, I have produced, peer-reviewed, and published research in areas such as fingerprinting, anomaly detection, multifactor authentication and embedded systems security. In many of these cases, I focused not only on designing novel security systems but also on designing usable web-based security systems for controlling them and understanding their data output. In fact, some of my research has formed the basis for commercial products and services. For example, in my work on integrated audit and access control, which was funded in part by Accenture Labs, I developed a Hadoop-

based application to perform large-scale statistical analysis of audit logs from an electronic medical record system. As part of this work, I also designed a web application to automatically produce human-readable reports and graphs for use in consulting. The system I designed is able to discern implicit access models in a hospital and to then audit EMR use based on these models in order to detect potential HIPAA violations. Accenture subsequently patented this technology.

11. Similarly, in my work at Applied Communication Sciences in 2013, I designed and implemented a web-based traffic visualization dashboard and analysis system for field area smart grid networks that could be used to quickly gain an understanding of the current state of a SmartGrid network as well as to detect unexpected anomalies in the network. Applied Communication Sciences subsequently patented this work and continued to build on the project. To my knowledge, they actually sold and/or still sell this product as part of their SecureSmart Managed Security Service product offering.

12. I have worked on and published two research projects related to improving the quality and ease-of-use of authentication technologies in healthcare settings. In one project, I and my co-authors designed a cryptographic security system for wireless technology used in medical networks. The result was an indoor location tracking system consisting of unspoofable Bluetooth Low Energy beacons. These beacons were placed around a building and mapped to a backend such that a user could report which beacons he or she was within range of in order to be used as a secondary authentication mechanism for accessing patient medical records. In the way that we designed and envisioned the system, a doctor would log into a mobile device which would connect to a web-based backend. As the doctor walked past patient rooms, he or she would be automatically presented with medical

records of nearby patients. In another project, I and my co-authors designed an authentication bracelet for doctors that would receive a Kerberos ticket upon login to a modified computer terminal through use of low-energy electrical signals transmitted over the wearer's skin. When using other hospital terminals, this Kerberos ticket could be sent back over the wearer's skin to the custom contact on the terminal in order to allow the doctor to login without a password. The bracelet was also designed to immediately lose the cryptographic secret upon being removed from the user. This allowed doctors to authenticate to a computer on wheels terminal at the beginning of their shift and then to subsequently authenticate themselves in various other contexts as they went about their shift merely by touching specially designed access panels.

13. My recent research has focused primarily on embedded systems security with an emphasis on binary analysis, anomaly detection, and automated security enforcement. Some of this research has focused on reverse engineering embedded medical devices to add novel security monitoring technology onto insecure devices. This security system can be soldered directly to the CPU of the medical device in order to perform control-flow integrity for purposes of profile building and enforcement. Such techniques prevent against control-flow hijacking attacks as well as physical attacks that leverage configuration modes to change device settings. In another case, I designed a system to automatically discern name and version information from binaries on embedded devices in order to build a software profile of the platform configuration of the device, which can then be cross-referenced with a vulnerability database. I have also written a patent on this specific technique.

14. In February 2016, I joined Harbor Labs full-time as a research scientist. In January 2019, I was promoted to senior research scientist. At Harbor Labs, I manage client engagements and lead teams in the areas of security analysis and source code analysis.

15. As part of my work at Harbor Labs, I have worked on the design and implementation of cryptographic protocols for securing data in medical devices. As another part of my work, I have worked with companies to reverse engineered their medical devices to discover and exploit previously unknown vulnerabilities.

16. A substantial portion of my role at Harbor Labs is supervising source code review teams as part of legal consulting engagements. As part of this work, I have reviewed software systems of varying sizes, often totaling in the millions or billions of lines of code. I have reviewed products in the security space, television-based set top boxes, network appliances, numerous web-based enterprise systems, email management systems, telephony products, embedded system bootloaders, social network platforms, and countless other products. I have conducted and/or supervised source code reviews in more than 48 cases.

17. I am also the technical and development lead for a firmware security analysis engine for a product that we are developing called Firmware IQ. In this role I perform experiments, write source code in Python, review the source code written by others, and supervise documentation and testing efforts.

II. SCOPE OF ENGAGEMENT

18. I understand that Surgical Instrument Service Company, Inc. (hereafter SIS) contends that Intuitive Surgical, Inc. (hereafter Intuitive) has engaged in allegedly anticompetitive behavior by using cryptographic controls on EndoWrist devices.

19. I have been asked to review the report of Mr. Kurt Humphrey and to provide my opinions on the subjects he covers. I have also been asked to provide my own, independent opinions on the security concerns with respect to RFID systems, the reasons for encrypting them, and the risks associated with not doing so. I also have been asked to opine on the differences between the chips used in different generations of EndoWrists and the advantages of the RFID system over the previous generation of technology. Finally, I have been asked to opine on the differences of reverse engineering wired and wireless chips.

III. SUMMARY OF OPINIONS

20. It is my opinion that wireless systems, including the RFID system used in certain EndoWrist Instruments compatible with the X/Xi da Vinci Surgical Systems (referred to throughout as "X/Xi instruments" or "X/Xi EndoWrists"), have additional security concerns related to the wireless nature of the communication that differentiate them from wired systems. To attack a wired system, an attacker generally must have close physical proximity to the system, and the attacker is thus more susceptible to physical security controls. Unlike a wired system, a wireless system must contend with attackers that do not require direct physical access to the system, but who are either within radio range of the system or have placed equipment within range of the system. Due to these concerns, wired systems require cryptographic controls in order to provide a similar level of data security to a system with a direct physical connection.

21. It is my opinion that the encryption Intuitive employed on the X/Xi instruments is consistent with these risks and reflects best practices to protect the data contained on or transmitted through the RFID system from being intercepted or altered. The RFID chip

encryption protects not only the use counter information on the X/Xi instruments but also the tool user ID, instrument drive parameters, and calibration data for the instrument.

22. It is my opinion that the Atmel RFID chip used in the X/Xi instruments offers substantive improvements over the DS2505 chip used in previous generations of EndoWrist Instruments compatible with the S/Si da Vinci Surgical Systems (referred to throughout as "S/Si instruments" or "S/Si EndoWrists"), including increased memory, faster data access, and improved reliability and endurance.

23. Furthermore, it is my opinion that a wireless communication channel offers general improvements over a wired communication channel. Wired technology requires special care and attention in the design and manufacturing process, to prevent against accidental damage and to ensure that physical strain is minimized. In contrast, wireless technology has lower manufacturing complexity, and it has increased reliability against physical damage. This is especially useful in systems such as an EndoWrist where physical mobility has the possibility of damaging or disconnecting the wire, reducing reliable operation of the device.

24. It is my opinion that Mr. Humphrey's [redacted] for consistency with the Humphrey report) is substantively flawed in that it ignores [redacted]

25. Finally, it is my opinion that reverse engineering the X/Xi instruments involves a different process than reverse engineering the S/Si instruments, though Mr. Humphrey's

analysis on the extent of the time and resources needed to reverse engineer the X/Xi instruments is speculative.

IV. BACKGROUND ON CYBERSECURITY AND CRYPTOGRAPHY

26. Security is the process of preventing unauthorized third-party access to protected data and privileged devices or, more generally, system functionality.

27. When considering a system's security, it is not enough to merely list all of the security controls in place. One must consider how users use the system. One must also evaluate attackers in terms of goals, capabilities, and return on investment. That may require assessing an attacker's potential motivation, whether they would require sophisticated hardware, what information would be accessible, how many users would be impacted from an attack, whether an attack would be costly, and other factors specific to a given system. The context of a system's use can greatly influence the answers to these questions as a security system in one context may be grossly insecure compared to the same system in another context. For example, a security analysis of a laptop requires an understanding of how the system is accessed, who accesses it, when and where they access it, and how and where data is stored. These details give insight into the threat model.

28. A threat model formalizes security risks to the system by enumerating vulnerabilities, weaknesses, and defects, and considers the risk of those defects if exploited by an attacker. It is industry best practice for device manufacturers to perform a formal security analysis, including a threat model, of a product before bringing it to market. A threat model formally defines attackers in terms of goals, capabilities, and relation to the system.

29. While a threat model exposes security risks, security requirements or controls address and reduce these risks. In other words, security requirements prescribe how a device should be secured to reduce the risks identified in the threat model. Typical security requirements include access controls to limit the exposure of data and functionality and the use of standardized cryptographic algorithms and protocols to protect data at rest and in transit via a network.

30. Cryptography is the study of how to hide information. It is often used to secure or protect electronic communication between entities. Cryptography includes two general methods for altering the readability of information: encryption and decryption. Encryption is the practice of converting readable information into unreadable information through use of a key; decryption is the inverse. Those skilled in the art refer to readable information as plaintext and encrypted information as ciphertext. In theory, by encrypting private data, an attacker without the decryption key will only have access to the ciphertext, which does not leak any data, thus keeping the data confidential.

V. SECURITY VULNERABILITIES OF WIRELESS SYSTEMS AND ENCRYPTION AS A MITIGATION MEASURE.

31. I understand that Intuitive has produced different generations of EndoWrist instruments over the years. These include the IS2000 and IS3000 (S/Si) instruments and IS4000 (X/Xi).[1] [redacted] While the EndoWrist S/Si instruments use a direct wired connection for communication between the da Vinci Robot and the EndoWrist, the

[1] Duque Dep. Tr. ("Duque") at 23:25–24:19.
[2] Somayaji Dep. Tr. at 128:1–10.

EndoWrist X/Xi instruments use a wireless connection over an RFID interface to send identification information, instrument drive parameters, calibration, and use counts from the EndoWrist X/Xi to the da Vinci robot.[3]

32. Wired connections have different security considerations than wireless connections. Although there are numerous security considerations besides just the connection between the da Vinci Robot and EndoWrist, I limit the following discussion to security considerations with respect to this connection only, so that I can more easily compare this aspect of the system design.

33. A da Vinci Robot using a wired connection to an S/Si EndoWrist has different security concerns and a different threat model than a da Vinci Robot using a wireless connection to an X/Xi EndoWrist. The threat model with respect to the wired connection is simpler than the threat model with respect to the wireless connection.

34. An important threat consideration for a wired connection is an attacker with direct physical access to the system. In the absence of mitigation measures, an attacker with physical access can tamper with the connection between the da Vinci Robot and the S/Si instruments. For instance, a passive attacker can eavesdrop on the physical connection by tapping it, in order to observe the data sent across. An active attacker also could intercept and change the data. In both cases, the attacker generally must have close physical proximity to the da Vinci system when attacking a wired system, and is therefore more susceptible to physical security controls such as security guards and security camera monitoring.

[3] Duque 30(b)(6) Dep. Tr. ("Duque 30(b)(6)") at 20:7–21:5; Somayaji Dep. Tr. at 109:6–22.

35. That is to say, for the wired connection of the S/Si EndoWrists, the threat model would contain adversaries in the classes "passive physical attacker" and "active physical attacker."

36. In contrast to the threat model of the S/Si EndoWrists where system communications occur through a direct physical connection, the X/Xi EndoWrists use a wireless connection between the da Vinci Robot and the EndoWrist to convey via radio frequency ("RF") certain system communications, including identification information, instrument drive parameters, calibration, and use counts.[4]

37. Therefore, for the wireless system, the threat model is a superset of the threat model for the wired system. The model must be expanded to also include nearby attackers (both active and passive) within radio range. A wireless system like the radio frequency identification ("RFID") system in the X/Xi systems not only has to contend with active and passive attackers, it also needs to consider the possibility that an attacker does not have direct physical access to the da Vinci system but is either near the robot (within radio range) or has placed equipment near the robot and is thus able to perform the attack on the RF communication channel without a nearby physical presence.

38. To provide a comparison, a typical computer network may be wired, wireless, or both. In a wired network that uses CAT5-7 or fiber optic cabling, security concerns are primarily related to physical attackers. Therefore, wired network connections typically do not leverage link-layer encryption because administrators are not worried about wireless attackers eavesdropping on the connection to observe the data sent across. On the other

[4] Somayaji Dep. Tr. at 56:4–60:9.

hand, computers on wireless networks broadcast all of their data publicly in order to enable communication between the access point and the endpoint. Because all wireless networking equipment sharing a particular standard implementation (*e.g.* 802.11ac) is able to communicate with all other such equipment, an attacker can easily eavesdrop on communications between any client and a base station.

39. For this reason, encryption is used to ensure privacy and integrity of communications on wireless networks. Originally, the first widespread encryption standard for Wi-Fi networks was called WEP, which stood for "wired equivalent privacy." Later encryption standards are named "Wi-Fi protected access." As the name implies, the purpose of this form of encryption is to provide protection to the wireless communication channel of similar quality to a wired communication channel.

40. In order to provide a similar level of security to the direct physical connection for the S/Si instruments, the X/Xi instruments must provide additional security controls to protect against attacks that specifically affect wireless communication channels like the RFID at issue here. Without appropriate mitigation measures, wireless communication channels can be susceptible to a number of attacks.

41. One example of such an attack is a passive eavesdropping attack.[5] As with the Wi-Fi example discussed above, it is trivial for an attacker with RFID equipment to read an RFID tag if the communication is not encrypted because, like Wi-Fi, RFID is an open standard. Indeed, attackers can purchase inexpensive RFID tools online.[6] If the

[5] Grassi et. al., *Digital Identity Guidelines*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, June 2017 at 45-46, 50, available at: https://doi.org/10.6028/NIST.SP.800-63-3

[6] RFID Readers, AMAZON, available at https://www.amazon.com/RFID-Readers/s?k=RFID+Readers (last visited Jan. 18, 2023); Intuitive-00506505 at -6593.

communication channel is not encrypted, such inexpensive tools can be used to intercept and read the data transmitted between the X/Xi instruments and the robot. The range of most RFID tools can be extended through the use of a more powerful antenna, so the attacker need not be in the same room as the system, making physical security measures – like controlled access areas for use of the robot or spotting an attacker in the room – ineffective.[7]

42. It is also possible to perpetrate active RFID attacks through the use of programmable RFID emitter features of these same tools.[8] Active RFID emitters can have a range of hundreds of meters.[9] These emitters can be programmed to broadcast arbitrary RFID values. In some cases, they can be used in impersonation attacks in which they impersonate another, unsecured, RFID tag.

43. The attacker need not be in the same room or even the same city to perpetrate these types of attacks on an unencrypted RFID channel, as the range of RFID communication can be extended. One such method can be performed by connecting RFID equipment to a small local computer with a connection to a longer-range network such as the Internet. The local computer can then be programmed to send observed RFID tag values to a remote computer over a secure channel such as SSH connection.[10] The remote computer can

[7] GITHUB, *Proxmark3*, available at: https://github.com/Proxmark/proxmark3 (last visited Jan. 18, 2023).
[8] Grassi et. al., *Digital Identity Guidelines*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, June 2017 at 39, 48 available at: https://doi.org/10.6028/NIST.SP.800-63-3; Tyler Petersen, *RFID Card Security and Attacks*, (Oct. 15, 2020), SIKITCH, available at: https://www.sikich.com/insight/rfid-card-security-attacks-and-prevention/#:~:text=An%20MITM%20attack%20against%20an,gain%20access%20to%20the%20building.
[9] Annalee Newitz, *The RFID Hacking Underground*, WIRED, (May 1, 2006), available at: https://www.wired.com/2006/05/rfid-2/.
[10] OPENSSH, available at: https://www.openssh.com/ (last visited Jan. 18, 2023).

also control the RFID equipment on the local computer to perpetrate active attacks using the same type of a connection. Such attacks are known as range-extension attacks.

44. A similar and related concept is the concept of impersonating, "spoofing"[11] or "cloning"[12] an RFID tag value. A spoofed RFID tag impersonates another RFID tag by broadcasting the same value as the tag. In many applications, spoofing is not a concern, but in certain types of systems such as RFID-based tracking systems, spoofing is a security issue.

45. Another type of common attack unencrypted wireless channels are susceptible to, is a replay attack.[13] In such an attack, an attacker reads an RFID value and later plays the same value back to a receiver at a different time. In some systems, RFID values change or rotate according to a time schedule. A replay attack allows an attacker to "play back" an earlier tag at a later time. Depending on the design and security of the system, this may allow the attacker to "replay" a value that allows some specific type of access to the system associated with that particular value.

46. I have personally designed and published research on novel anti-spoofing and anti-replay attack-related wireless security systems.[14]

[11] KASPERSKY, *What is Spoofing - Definition and Explanation*, available at: https://www.kaspersky.com/resource-center/definitions/spoofing (last accessed Jan. 18, 2023).
[12] Tyler Petersen, *RFID Card Security and Attacks*, (Oct. 15, 2020), SIKITCH, available at: https://www.sikich.com/insight/rfid-card-security-attacks-and-prevention/#:~:text=An%20MITM%20attack%20against%20an,gain%20access%20to%20the%20building.
[13] Grassi et. al., *Digital Identity Guidelines*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, June 2017 at 53, available at: https://doi.org/10.6028/NIST.SP.800-63-3
[14] Martin et. al., *Applications of Secure Location Sensing in Healthcare*, Proceedings of the 7th ACM International Conference on Bioinformatics, Computational Biology, and Health Informatics (2016).

47. The wireless attacks above are not generally applicable to wired systems in the same manner I described above. While it is possible for an attacker to perpetrate such an attack in a wired system, it is more difficult as physical access is required. Therefore, it is important to specifically consider wireless attacks in the design of a wireless system.

48. One way to prevent many types of wireless attacks is through use of cryptographic controls. For example, passive RFID attacks can be prevented by encrypting the tag data. Similarly, encryption or authentication of the tag data can be used to prevent a system from interpreting a false tag data as being from a trusted source.

49. Range extension attacks cannot be prevented entirely through use of cryptography, but their effectiveness can be reduced because an attacker cannot tamper with a cryptographically protected value without knowing the underlying encryption key.

50. Given that Intuitive wirelessly broadcasts essential data—including its counter code and calibration data—using an RFID system in the X/Xi instruments,[15] in my opinion it is both reasonable and necessary to protect that information using cryptography in order to provide a similar level of security to the direct physical connection used to transmit similar information for the S/Si instruments. Further, it is my opinion that it would be illogical to broadcast a counter code that is unprotected, as an unreliable or inauthentic counter code would serve little purpose.

51. The FDA's inquiries to Intuitive emphasize the importance of encryption in preserving wireless data protection and integrity. I understand that the FDA is increasingly focused

[15] Somayaji Dep. Tr. at 56:4–57:23.

on cybersecurity during the review of submissions, and the lack of cybersecurity measures could generate major deficiencies.[16]

52. Consistent with these requirements, the FDA specifically inquired into Intuitive's cybersecurity risk assessment for the X/Xi system, including Xi/Xi instruments. In a submission to the FDA, Intuitive provided its risk assessment that identified a number of identified cybersecurity risks and the mitigation measures Intuitive employed to reduce the likelihood or severity of those risks.[17] One identified risk associated with the RFID reader was that the "[c]ompromise of interface leads to modification of instrument/scope data or injection of false instrument/scope data."[18] The consequences of that type of compromise were listed as (1) "[m]odification of instrument/scope parameters can cause incorrect motion control" and (2) "[p]ossible to use surgical instruments beyond tested life." Both were listed as "Critical" severity, defined as "[c]ompromise of interface can lead to minor or significant surgical or clinical intervention, and results in reversible harm to the patient or user."[19] As a mitigation measure for this identified risk, Intuitive stated, "Communications between RFID reader and tag are encrypted."[20] That reduced the likelihood of the identified risk occurring to "improbable," resulting in a post-risk index of "III: Tolerable Risk."[21] Another identified risk was associated with the RFID tag and described as, "[m]odification of instrument/scope data or injection of false instrument/scope data."[22] The consequences of a compromise of this data were identified

[16] Expert Report of Christy Foreman (Jan. 18, 2023), ¶¶ 246-254.
[17] Intuitive-00499468 at -9640; Intuitive-00506505.
[18] Intuitive-00506505 at -6542.
[19] *Id.* at -6536.
[20] *Id.* at -6542
[21] *Id.*
[22] *Id.*

as follows: (1) "[m]odification of instrument/scope parameters can cause incorrect motion control" and (2) "[p]ossible to use surgical instruments beyond tested life."[23] These consequences also received a "Critical" severity rating.[24] Two mitigation measures were identified that reduced the likelihood to "Improbable" and the post-risk index to "III: Tolerable Risk": (1) "[d]ata on RFID tag are encrypted and password-protected" and (2) "[e]ncryption key and use counting data areas on RFID tag are one-time programmable and cannot be modified once written."[25]

53. This is consistent with my opinions regarding the importance of encryption on wireless communication channels, including the RFID system in the X/Xi instruments, for data of this nature. In testing their RFID security, [redacted][26] Considering the widespread availably of wireless hacking instruments and the motion control and use counter data stored on Intuitive's RFID chip, the risks of leaving Intuitive's RFID chips unencrypted warranted mitigation steps to reduce the likelihood of those potentially critical risks occurring. [redacted][27] [redacted][28]

[23] Intuitive-00506505 at -6542.
[24] *Id.*
[25] *Id.*
[26] *Id.* at -6593.
[27] *Id.* at -6594.
[28] *Id.*

VI. THE ATMEL CRYPTORF EEPROM CHIP USED IN THE X AND XI ENDOWRISTS OFFERS SUBSTANTIVE IMPROVEMENTS OVER THE DS2505 EEPROM CHIP

54. In paragraphs 37-59 of his report, Mr. Humphrey purports to explain the reason that Intuitive switched from the wired DS2505 chip in the S/Si EndoWrists to the wireless Atmel chip in the X/Xi EndoWrists.[29] He concludes that the primary purpose of this change was to prevent third parties from adding lives to the X/Xi EndoWrists. As a threshold matter, it would have been entirely possible for Intuitive to add more advanced cryptography to the EndoWrist in a wired design. Switching to a wireless RFID design thus would be unnecessary if the only goal was to provide enhanced cryptographic security to the use counter.

55. In paragraph 38 of his report, Mr. Humphrey reports that, "evidence has not been identified that the Atmel RFID chip offers any substantive improvement over the existing DS2505 chip in operational performance of the X/Xi system."[30] Mr. Humphrey also speculates that the only reason that Intuitive would have made this change is to stop third-party companies from altering the devices.[31]

56. However, evidence of a substantive improvement in the Atmel RFID chip is apparent from a comparison of the data sheets for the two chips. A comparison of the relevant data sheets for the DS2505[32] and the Atmel CrpytoRF[33] chips shows numerous key difference and benefits to the Atmel CryptoRF chip including:

---

[29] Expert Report of Kurt Humphrey (May 10, 2021), ¶¶ 37-29.
[30] Expert Report of Kurt Humphrey (May 10, 2021), ¶¶ 38.
[31] Expert Report of Kurt Humphrey (May 10, 2021), ¶¶ 47-54.
[32] Dallas Semiconductor DS2505 Data Sheet.
[33] Intuitive-00999731 (Somayaji Deposition, Ex. 224) - Atmel CryptoRF EEPROM Memory Summary Datasheet; Atmel CryptoRF EEPROM Data Sheet.

i. Configuration options for more memory: The Atmel CryptoRF chip is available in more memory configurations and larger memory configurations than the DS2505 chip. This allows for more data to be stored and transferred either as part of the design of the EndoWrist X/Xi or, if not used in this context, allows for easier upgrades in later EndoWrist models that might want to store and transmit more data.

i. Better security features: The Atmel CryptoRF chip supports a range of stronger security features.

ii. High-reliability/high endurance: The CrytpoRF chip advertises a high endurance and high reliability design including 100,000 writes and 10 year data retention. In contrast, the DS2505 data sheet does not list any particular reliability or endurance guarantees.

ii. Integrated tuning capacitor: Unlike the Dallas Chip, the Atmel CryptoRF chip advertises an integrated tuning capacitor.

The Atmel chip also offers up to four times as much storage space and nearly twice as fast data access times than the Dallas chip.[34]

57. Mr. Humphrey also ignores the benefits of wireless technology versus wired technology entirely in his analysis. Wireless technology has numerous benefits over wired.

58. Wired technology requires special care and attention to ensure that wires are routed appropriately in order to minimize repetitive mechanical strain on them (which can cause wires to break over time) and to prevent accidental damage. Similarly, wired technology

[34] Intuitive-00544903 at 5094.

requires special design in connection points, such as where an EndoWrist connects to a da Vinci Robot, in order to ensure that the wire cannot inadvertently become disconnected during use. Wires must also be shielded to prevent RF interference and care must be taken to ensure that they are not defective and that they are connected securely.

59. In contrast, wireless technology has increased reliability against physical damage, as there is no wire that can accidentally break or become disconnected. Wireless technology also tends to have lower manufacturing complexity, as physical concerns related to connecting and routing wiring need not be addressed. This is especially useful in systems such as an EndoWrist where physical mobility has the possibility of damaging or disconnecting the wire or other physical components, reducing reliable operation of the device.[35]

60. Mr. Humphrey dismisses all advantages of wireless chips as "insignificant" in part because Intuitive apparently considered the Dallas Chip as a back-up option. Mr. Humphrey states that, "[o]n the contrary, any possible, yet unstated, performance advantages that might have been anticipated by introducing the RFID chip were insignificant enough that Intuitive used the conventional Dallas chip as their contingency or back-up plan in the event the RFID chip design change failed…the X/Xi EndoWrist module was designed to use either the Dallas chip or the RFID chip without further modifications. Therefore, it appears unlikely that the resulting EndoWrist operational or

[35] Somayaji Dep. Tr. at 81:7-11; Intuitive-00538994 at Tab 19.

mechanical performance would be substantially different, or even distinguishable, regardless of which chip was used."[36]

61. It is my experience that a "fallback" option that exists in case of a supply shortage or other contingencies does not necessarily provide the same performance as the original option. In many cases, the fallback option is compatible, but is lower performing, which is why it is designated as a fallback and not an alternative main option.

62. Furthermore, the conclusion that a fallback option must have insignificant differences to the original option is undermined by the fact that the DS2505 chip does not have RFID and the numerous other functionalities identified above. The "fallback" option therefore is not identical in terms of feature set, and it is unreasonable to assume that the "fallback" option is not "distinguishable" in terms of performance.

63. In my experience, it is extremely common for chips to have the same external interface so that they would fit into the same mechanical design while offering differing performance. Computer central processing unit ("CPUs") are designed this way. For example, Intel supports numerous CPUs with massively differing performance (as determined by core counts, clock speed, overclocking, Turbo Boost, and SMT support) and features that are all pin-compatible with one another, meaning one chip can be directly substituted for another without any changes to the circuit or board layout.[37] Because all processors are pin-compatible it is possible that a slower processor could be used as a "fallback" option for a particular application if a desired model is unavailable. It does not follow that just

[36] Expert Report of Kurt Humphrey (May 10, 2021), ¶¶ 38-39.
[37] *Products Specifications*, INTEL, available at: https://ark.intel.com/content/www/us/en/ark/search/featurefilter.html?productType=873&1_Filter-SocketsSupported=3562 (last visited Jan. 18, 2023).

because the processors are pin-compatible that they have the same performance. Similarly, identifying the Dallas Chip as a "fallback" does not mean that it offered the same benefits as the RFID chip.

64. In paragraph 42 of his report, Mr. Humphrey cites a chart showing a higher instrument failure rate for the da Vinci Xi line of products compared to the da Vinci Si. But as Mr. Humphrey himself admits, "[t]he disclosed RMA/return data details are insufficient to draw any firm conclusions regarding reliability issues associated with replacement of the DS2505 chip in the S/Si EndoWrist instruments with the Atmel CryptoRF chip in the X/Xi EndoWrist instruments."[38] Furthermore, the data that Mr. Humphrey cites do not compare the DS2505 to the Atmel CryptoRF, and they represent a single point in time with no evidence identified by Mr. Humphrey that they would be representative of the entire product life cycle for the X/Xi instruments.

65. Finally, Mr. Humphrey speculates that Intuitive only cared about securing the use counter when making the decision to switch to an RFID interface. He bases this in part on his statement that when Intuitive received information on security concerns with the Atmel chip, "the only concerns [Intuitive] raised were 'about methods to reprogram our RFID's, i.e. change the life-count so that instruments get re-used beyond their design life…'"[39] However, this document appears to post-date the launch of the X/Xi EndoWrists with the RFID technology and the cyber risk assessment referenced above by many years.[40] In his focus on this single email chain reflecting on discussion, Mr. Humphrey ignores other documents, including the cyber risk assessment submitted to the FDA, that also identified

[38] Expert Report of Kurt Humphrey (May 10, 2021), ¶ 42.
[39] Expert Report of Kurt Humphrey (May 10, 2021), ¶ 55.
[40] Intuitive-00861667.

the need for encryption to protect other instrument parameter data that could lead to incorrect motion control of the instruments if compromised.[41]

66. Mr. Humphrey also cites another an email dated years *after* the launch of the X/Xi, where an Intuitive employee notes that "*another possible*" reason to move to X/Xi models is that, "companies have so far only done reprogramming on Si" and "we probably have lead time before they figure out X/Xi."[42] It is not clear how the email would inform or relate to a decision about encryption on a chip for the X and Xi, particularly when that decision substantially predated this email.[43]

VII. BESIDES THE USE COUNTER, THERE ARE OTHER ASPECTS OF THE X/XI ENDOWRISTS THAT USE CRYPTOGRAPHIC CONTROLS

67. There are other aspects of the X/Xi instruments, besides the use counter, that use cryptographic controls. For example, the RFID tag contains calibration information, which is needed for the da Vinci to perform its movements.[44] [redacted] [45] Furthermore, the Tool User ID (TUID) – a number coded for each instrument type – is also encrypted on the RFID chip. [redacted] .[47]

[41] Intuitive-00506505 at -6542.
[42] Expert Report of Kurt Humphrey (May 10, 2021), ¶ 52.
[43] Intuitive-00861667.
[44] Somayaji Dep. Tr. at 63:22–64:12.
[45] Somayaji Dep. Tr. at 110:10-23; Intuitive-00506505 at -542.
[46] Somayaji Dep. Tr. at 59:17–61:15.
[47] Duque 30(b)(6) Dep. Tr. at 40:22–41:1; Intuitive-00506505 at -6542; Somayaji Dep. Tr. at 60:15 - 61:15.

68. Furthermore, the ID was encrypted to both ensure that an unlocked device would not escape an Intuitive manufacturing facility thereby protecting the secrecy of the encryption strategy (a sound precaution if cryptography is to be used at all) and to prevent the data in the RFID from becoming corrupted. [48]

VIII. MR. HUMPHREY'S ANALYSIS OF [redacted] CONTAINS ERRORS AND [redacted]

69. Mr. Humphrey contends that [redacted]

[redacted]

[redacted]

[redacted]"[49] Mr. Humphrey then cites the following chart:

[redacted]

[48] Intuitive-00994614.
[49] Expert Report of Kurt Humphrey (May 10, 2021), ¶ 56.

[redacted]

70. He also cites deposition testimony in which [redacted].[50] Mr. Humphrey then states, [redacted] For example, [redacted]

71. There are numerous issues in Mr. Humphrey's analysis. As a threshold matter, [redacted]

[50] Expert Report of Kurt Humphrey (May 10, 2021), ¶ 56.
[51] Expert Report of Kurt Humphrey (May 10, 2021), ¶ 57.

[redacted][53]

[redacted]

72. Furthermore, it is not clear that Mr. Humphrey has identified [redacted] Specifically, the deposition testimony that Mr. Humphrey cites [redacted] That is consistent with [redacted]"[55] It is also consistent with an [redacted]

[52] Intuitive-01004385 at -4388.
[53] *Id.*
[54] *Id* at -4389.
[55] Intuitive-01004232 at -4236.

[redacted][56]

73. Finally, I understand this relates to an [redacted] In my opinion, it is highly improper to review [redacted] and then to draw conclusions [redacted]

IX. REVERSE ENGINEERING X/XI INSTRUMENTS INVOLVES A DIFFERENT PROCESS THAN REVERSE ENGINEERING S/SI INSTRUMENTS.

74. In my opinion, reverse engineering X/Xi instruments involves a different process than reverse engineering the S/Si instruments. Because the X/Xi instruments employ a different security method than the S/Si instruments, the reverse engineering process is also substantially different.[58] This process requires a more sophisticated analysis.

[56] Intuitive-01004242, at -4243.
[57] Expert Report of Christy Foreman (Jan. 18, 2023), ¶¶ 119, 246-254.
[58] Somayaji Dep. Tr. at 109:25-110:6.

Reverse engineering the data stored in a wired chip that lacks encryption does not involve a decryption process, and would instead be more easily accomplished using passive eavesdropping techniques.

75. Though the processes are different, in my opinion, Mr. Humphrey's contentions regarding the extent of the difficulty of reverse engineering the X/Xi instruments are speculative. Mr. Humphrey's analysis appears to be based on a review of documents. Documents may not accurately or fully reflect all implementation details of a device. In my opinion, estimates on reverse engineering difficulty are much more accurate after examining a physical device and attempting to reverse engineer it, and they would vary based on the technical skills and tools used by the engineer. Mr. Humphrey's estimates are not representative of an industry-wide sample, and they do not account for differences in training, experience, or expertise in the reverse engineers engaged in this undertaking.

76. Although I do not attempt to canvas them all here, Mr. Humphrey's July 26, 2021 report, which he calls his "Rebotix Report" and incorporates by reference in Paragraph 19, contains a number of key methodological flaws, one of which undermines his entire analysis.[59] In his Rebotix Report, which forms the basis of how Mr. Humphrey opines that Rebotix would access and reset the Xi use counter, Mr. Humphrey's analysis is predicated on the fact that the data stored on the X/Xi chip is not encrypted at rest.[60]

---

[59] Expert Report of Kurt Humphrey (July 26, 2021) (submitted in the matter of *Rebotix Repair LLC v. Intuitive Surgical, Inc.*, Case No. 8:20-cv-02274 (M.D. Fla.) ("Humphrey Rebotix Report").

[60] For example, Paragraphs 39-41 describe methods to extract a clean image of the data on the CryptoRF chip. Mr. Humphrey then states, "[s]uccessful extraction and analysis of clean images from the CryptoRF EEPROM facilitates straightforward editing/rewriting of the use count and reprogramming an existing X/Xi EndoWrist CryptoRF EEPROM or replacing the existing CryptoRF EEPROM with a new CryptoRF EEPROM personalized with the edited image file." *See* Humphrey Rebotix Report at ¶ 43. Mr. Humphrey also writes, "[t]he user data stored in the Atmel RFID chip can be optionally access and password protected but there is no provision for encrypting stored data internal to the EEPROM block. As

77. However, that premise is not consistent with Intuitive documentation, nor is it consistent with statements made elsewhere in Mr. Humphrey's report. As Mr. Humphrey recognized elsewhere in his report, Intuitive documentation states that the "[d]ata on RFID tag are encrypted and password-protected," and that the "[e]ncyption key and use counting data areas on RFID tag are one-time programmable and cannot be modified once written."[61]

78. Since Intuitive's own documentation and Mr. Humphrey's report contradict the major assumption that Mr. Humphrey's entire reverse engineering analysis depends upon, his analysis is incorrect and his methodology is faulty and unlikely to succeed in practice.

X. CONCLUSION

79. In conclusion, it is my opinion that wireless systems have different security concerns than wired systems, and thus it is necessary to use cryptographic controls on wireless systems to ensure data integrity and security from attackers without a physical presence in the room. Wireless systems have general benefits over wired systems, and specifically the Atmel RFID chip used in the X/Xi EndoWrist X and Xi offers substantive benefits over the DS2505 chip besides the encryption of the use counter. Mr. Humphrey's analysis of the [redacted] is improper because it is [redacted]. Although reverse engineering the X/Xi instruments involves a different process than reverse engineering the S/Si instruments, Mr. Humphrey's analysis is speculative and contains methodological flaws.

previously stated, the only encryption capability available on the CryptoRF chip is during password transmission (through the Authentication Communication setting) and password/user data transmission (through the Encryption Communication mode)." *See* Humphrey Rebotix Report at ¶ 27.

[61] Humphrey Rebotix Report at ¶ 23; Intuitive-00506505 at -6542.

***

All of the facts stated in this report are known personally to me and the opinions proffered are my own. If called as a witness, I could and would testify competently thereto. I declare under penalty of perjury of the laws of the United States that the foregoing is true and correct to the best of my knowledge.

January 18, 2022

Paul D. Martin, Ph.D.

Attachment A

Curriculum Vitae of Paul D. Martin

harborlabs
CYBER.SCIENCE

Paul D. Martin, Ph.D.

443.449.9006
paul@harborlabs.com
1777 Reisterstown Road, East Bldg, Suite 230; Pikesville, MD 21208

Profile

Dr. Martin is the Director of Firmware Security and a Senior Research Scientist at Harbor Labs. His research interests include embedded system security, operating system security, vulnerability analysis, reverse engineering, network protocol analysis, applied cryptography, cryptanalysis and privacy-preserving protocols.

Education

2011-2016	*Ph.D. Computer Science Johns Hopkins University Baltimore MD* *Securing Medical Devices and Protecting Patient Privacy in the Technological Age of Healthcare*	
2011-2013	*M.S.E. Computer Science Johns Hopkins University Baltimore MD*	
2007-2011	*B.S. Computer Science Johns Hopkins University Baltimore MD*	

Industry Experience

2018-Present	*Harbor Labs*	**Director of Firmware Security, Senior Research Scientist**
2013-2018	*Harbor Labs*	**Research Scientist**
2011-2016	*Johns Hopkins University Health and Medical Security Lab*	**PhD Candidate, Research Assistant**
2013	*Applied Communication Sciences*	**Graduate Intern**
2011	(ICPSR) *University of Michigan Inter-university Consortium for Political and Social Research*	**Penetration Tester**
2009-2011	*Independent Security Evaluators*	**Security Intern**
2008-2010	(DRCC) *Johns Hopkins University Digital Research and Curation Center*	**Student Programmer**
2008	*Brandeis University Hardware Repair Shop*	**Freelance Programmer**

Teaching Experience

2015	*Introduction to Hardware Hacking*	**Instructor**
2012-2014	*Security and Privacy*	**Teaching Assistant**
2011	*Practical Cryptographic Systems*	**Course Assistant**

Publications

P. Mart n, D. Russe , M. Ben Sa em, S. Checkoway, A. Rub n, Sent ne : Secure Mode Prof ng and Enforcement for Embedded Systems, Proc. ACM/IEEE Internat ona Conference on Internet-of-Th ngs Des gn and Imp ementat on, (IoTDI 18).

P. Mart n, M. Rushanan, T. Tant o, C. Lehmann and A. Rub n, App cat ons of Secure Locat on Sens ng n Hea thcare. In the proceed ngs of ACM Conference of B o nformat cs, Computat ona B o ogy, and Hea th Informat cs (BCB 16).

harborlabs
CYBER.SCIENCE

J. Carr gan, P. Mart n, M. Rushanan, KBID: Kerberos Brace et Ident f cat on. In the Proceed ngs of F nanc a Cryptography and Data Secur ty (FC 16).

P. Mart n, M. Rushanan, S. Checkoway, M. Green, A. Rub n. C ass fy ng Network Protoco Imp ementat on Vers ons: An OpenSSL Case Study. Techn ca Report 13-01, Johns Hopk ns Un vers ty (December 2013).

P. Mart n, A. Rub n, and R. Bhatt , *Enforcing Minimum Necessary Access in Healthcare Through Integrated Audit and Access Control.* In ACM Conference on B o nformat cs, Computat ona B o ogy, and B omed ca Informat cs Hea th Informat cs Sympos um (BCB-HIS), (September 2013)

Patents

System and Method for automat ca y extract ng nformat on from b nary f es for use n Database Quer es	**US 10,762,214 B1**
System and method for network traff c prof ng and v sua zat on	**US 9,667,521 B2**
System and method for network traff c prof ng and v sua zat on (Pend ng)	**US 15/606,717**
System and method for network traff c prof ng and v sua zat on (Pend ng)	**WO 2015113036A1**
Hea thcare pr vacy breach prevent on through ntegrated aud t and access contro	**US 8,984,583 B2**
Hea thcare pr vacy breach prevent on through ntegrated aud t and access contro	**US 9,438,632 B2**

Current Research

Automated b nary vers on extract on for NVD cross-reference based on fuzzy match ng.
Automated ana ys s of vu nerab t es n conta ners and v rtua app ances.
Large-sca e compar son of nature and k nd of f rmware vu nerab t es across and w th n product c asses.

Expert Witness Engagements

Un ted States **v. Laffon Ellis**

Case:	Case # 2:19-cr-00369-DWA
Descr pt on:	Ana ys s re ated to re ab ty of spec f c types of computer zed DNA ana ys s n cr m na proceed ngs.
Serv ces:	Source code rev ew. Expert report draft ng.
Expert Test mony at Hear ng:	Monrov a, MD (December 20, 2021)

Sysmex Corporat on and Sysmex Amer ca, Inc. v. **Beckman Coulter, Inc.**

Case:	CA # 19-1642-RGA-CJB
Descr pt on:	L t gat on re ated to hemato ogy ana ys s mach ne patents.
Serv ces:	Source code rev ew. Expert report draft ng.
Expert Test mony at Depos t on:	Monrov a, MD (November 22, 2021)

CERTAIN ROUTERS, ACCESS POINTS, CONTOLLERS, NETWORKS MANAGEMENT DEVICES, OTHER NETWORKING PRODUCTS, AND HARWARE AND SOFTWARE COMPONENTS THEREOF

Case:	ITC Invest gat on No. 337-TA-1227
Descr pt on:	ITC Invest gat on re ated to patents on w re ess network handoff, network management and QoS techno og es.
Serv ces:	Source code rev ew. Va d ty and pr or art ana ys s. Expert report draft ng.
Expert Test mony at Tr a :	Wash ngton, DC (Ju y 28, 2021)
Expert Test mony at Depos t on:	Monrov a, MD (June 9-10, 2021)

Micro Focus, Inc. v. Insurance Serv ces Organ zat on

Case:	DE C v Act on # 15-252-RGA
Descr pt on:	L t gat on re ated to un censed use of runt me env ronments,

harborlabs
CYBER. SCIENCE

brar es and software comp ers.
Serv ces: Source code rev ew. B nary reverse eng neer ng and ana ys s. Aff dav t draft ng. Expert report draft ng.
Expert Test mony at Depos t on: Monrov a, MD (Feb 2, 2021)

loanDepot.com, LLC v. S gma Infoso ut ons, Inc.
Case: AAA Case # 01-18-0001-5821
Descr pt on: L t gat on re ated to software deve opment pract ces.
Serv ces: Source code ana ys s, exper mentat on, report draft ng.
Expert Test mony at Depos t on: Ba t more, MD (December 17, 2019)

Cypress Lake Software, Inc. v. Samsung E ectron cs Amer ca and De , Inc.
Case: Case # 6:18-cv-00030-RWS
Descr pt on: L t gat on re ated to nfr ngement of UX patents.
Serv ces: Source code ana ys s, report draft ng.
Expert Test mony at Depos t on: Ba t more, MD (Ju y 9, 2019)

Apple, Inc. Device Performance Litigation
Case: CA C v Act on # 18-md-02827-EJD
Descr pt on: L t gat on re ated to bus ness pract ces.
Serv ces: Techn ca ana ys s and expert reports on secur ty and techn ca aspects of mob e phone forens cs.

Ita an Ant trust Author ty v. **Apple, Inc.**
Case: PS/11309
Descr pt on: L t gat on re ated to bus ness pract ces.
Serv ces: Techn ca ana ys s and expert reports on secur ty and techn ca aspects of software update processes.

Carl Zeiss AG and ASML Netherlands B.V. v. N kon
Case: Case # 2:17-cv-07083-RGK (MRWx)
Descr pt on: L t gat on re ated to patents on mage detect on a gor thms.
Serv ces: Code rev ew of a gor thms re ated to mage process ng and detect on a gor thms. Dec arat on on aspects of source code rev ew process.

Dec s on Resources, LLC v. **Brigham Hyde, Precision Health Intelligence, LLC and Orr Inbar**
Case: MA C v Act on # 17-2834J
Descr pt on: L t gat on re ated to t me ne of software deve opment and m sappropr at on of trade secrets.
Serv ces: Source code and documentat on rev ew, t me ne deve opment. Aff dav t draft ng.

Litigation Support

WSOU Investments, LLC. v. M crosoft Corporat on
Case: Case # 1:18- 6:20-cv-00464-ADA, 6:20-cv-00460-ADA, 6:20-cv-00457-ADA,
Descr pt on: L t gat on re ated to patents on te ephony management systems and sk -based matchmak ng.
Serv ces: Source code rev ew and documentat on rev ew, va d ty ana ys s, nfr ngement ana ys s, report draft ng.

10Tales Inc. v. T kTok PTE. Ltd.
Case: Case # 1:18-cv-826-WCB
Descr pt on: L t gat on re ated to patents on user-adapted v deo streams.
Serv ces: C a m construct on ana ys s.

harborlabs
CYBER. SCIENCE

Carr ere v. **Symantec Corporation**

Case:	Case # 500-06-000894-176
Descr pt on:	C ass act on t gat on re ated to product secur ty.
Serv ces:	Source code rev ew, documentat on rev ew, report draft ng.

IOENGINE, LLC v. Ingen co, Inc.

Case:	Case # 1:18-cv-826-WCB
Descr pt on:	L t gat on re ated to patents on payment process ng systems.
Serv ces:	Source code rev ew and documentat on rev ew, va d ty ana ys s, nfr ngement ana ys s, report draft ng.

IOENGINE, LLC v. PayPa Ho d ngs, Inc.

Case:	Case # 1:18-cv-452-WCB
Descr pt on:	L t gat on re ated to patents on payment process ng systems.
Serv ces:	Source code rev ew and documentat on rev ew, va d ty ana ys s, nfr ngement ana ys s, report draft ng.

AGIS Software Deve opment LLC v. **Uber Technologies**

Case:	Case # 2:21-cv-00026-JRG-RSP
Descr pt on:	L t gat on re ated to patents on map over ays and messag ng systems.
Serv ces:	Source code rev ew.

F njan v. **Palo Alto Networks**

Case:	Case # 4:14-CV-04908-PJH
Descr pt on:	L t gat on re ated to patents on ma ware scann ng gateways.
Serv ces:	Inva d ty ana ys s, C a m construct on ana ys s, source code rev ew.

Huawe Techno og es Co. v. **Verizon Communications Inc.**

Case:	Case # 6:20-CV-00090
Descr pt on:	L t gat on re ated to patents on ma ware scann ng gateways w th c oud components.
Serv ces:	Source code rev ew, non- nfr ngement ana ys s.

Ep c Games, Inc. vs. **Apple, Inc.**

Case:	Case # 4:20-cv-05640-YGR-TSH
Descr pt on:	L t gat on re ated to bus ness pract ces.
Serv ces:	Document rev ew, nterv ews, report draft ng.

Ph ps North Amer ca LLC ; Kon nk ujke Ph ps N.V. vs. **Summit Imaging Inc.**

Case:	Case # 2:19-cv-01745-JLR
Descr pt on:	L t gat on re ated to th rd-party repa r serv ces.
Serv ces:	Source code rev ew, document rev ew, report draft ng.

California Physicians Service, Inc D/B/A Blue Shield of California vs. Hea thp an Serv ces Inc,

Case:	Case # 3:18-cv-3730
Descr pt on:	L t gat on re ated to software deve opment pract ces and breech of contract.
Serv ces:	Document rev ew, source code rev ew, report draft ng.

F njan v. **Qualys**

Case:	Case # 4:18-cv-07229-YGR
Descr pt on:	L t gat on re ated to patents on vu nerab ty assessment products.
Serv ces:	Inva d ty ana ys s, Non- nfr ngement ana ys s, source code rev ew, report draft ng.

F njan v. **Sonicwall**

harborlabs
CYBER. SCIENCE

Case:	Case # 5:17-cv-04467-BLF-HRL
Descr pt on:	L t gat on re ated to patents on ma ware scann ng gateways.
Serv ces:	Inva d ty ana ys s, Non- nfr ngement ana ys s, source code rev ew, report draft ng.

TecSec Inc. v. C sco and Orac e

Case:	Case # 1:10-cv-115 LO-TCB
Descr pt on:	L t gat on re ated to patents on hardware acce erated cryptograph c processors.
Serv ces:	Infr ngement ana ys s, va d ty ana ys s, source code rev ew, report draft ng.

Blackberry Limited v. Facebook, Inc.

Case:	Case # 2:18-cv-01844-KSx
Descr pt on:	L t gat on re ated to patents on agent-based network mon tor ng, conf gurat on and secur ty systems.
Serv ces:	Infr ngement ana ys s, va d ty ana ys s, source code rev ew, report draft ng.

Un oc, Inc. v. **Big Fish Games, Inc.**

Case:	Case # 2:16-cv-00741-JRG
Descr pt on:	L t gat on re ated to patents on hardware cryptograph c ch ps.
Serv ces:	Non- nfr ngement ana ys s, report draft ng, source code rev ew.

SPEX Techno og es, Inc. v. **Toshiba America Electronic Components, Inc., et al.**

Case:	Case # 8:16-cv-01800-JVS
Descr pt on:	L t gat on re ated to patents on hardware cryptograph c ch ps.
Serv ces:	Non- nfr ngement ana ys s, report draft ng.

Symantec Corporation v. Zsca er, Inc.

Case:	Case # 3:17-cv-04414-JST,
Descr pt on:	L t gat on re ated to patents on secur ty gateways, URL f ter ng and categor zat on
Serv ces:	Infr ngement ana ys s, ass gnor estoppe , document rev ew.

Kon nk jke Ph ps v. **Microsoft Inc.**

Case:	Case # 4:18-cv-01885-HSG,
Descr pt on:	L t gat on re ated to patents on secure cryptograph c protoco s
Serv ces:	Non- nfr ngement ana ys s, va d ty ana ys s, c a m construct on ana ys s, document rev ew, source code rev ew.

Netfuel, Inc. v. C sco Systems, Inc.

Case:	Case # 5:18-cv-2352-EJD
Descr pt on:	L t gat on re ated to patents on agent-based network mon tor ng, conf gurat on and secur ty systems.
Serv ces:	Infr ngement ana ys s, c a m construct on ana ys s, source code rev ew, report draft ng.

Byrd et al. v. Aaron s, Inc., et a .

Case:	PA C v Act on # 1:11-cv-00101-SJM-SPB
Descr pt on:	C ass act on t gat on re ated to pr vacy.
Serv ces:	Attend depos t ons, source code rev ew, report draft ng.

F njan v. **Juniper Networks**

Case:	Case # 3:17-cv-05659-WHA
Descr pt on:	L t gat on re ated to patents on ma ware scann ng gateways.
Serv ces:	Inva d ty ana ys s, non- nfr ngement ana ys s, source code rev ew.

harborlabs
CYBER. SCIENCE

Grace et a . v. **Apple Inc.**

Case:	Case # 5:17-cv-00551-LHK (NC)
Descr pt on:	L t gat on re ated to dev ce performance and serv ce outages.
Serv ces:	Mob e forens cs and dev ce ana ys s, report draft ng, source code rev ew, document rev ew, techn ca ana ys s and argument construct on.

Rimini Street, Inc. v. Orac e Internat ona Corporat on, et a .

Case:	Case # 2:14-cv-01699 LRH-CWH
Descr pt on:	L t gat on re ated to fa se c a ms on secur ty.
Serv ces:	Large-sca e test ng of IPS techn ques for nc ud ng custom test nfrastructure and mp ementat on of techn ques to b ock exp o tat on of vu nerab t es, techn ca ana ys s of vu nerab t es.

F njan v. **Symantec Corporation**

Case:	Case # 14-cv-02998-HSG
Descr pt on:	L t gat on re ated to patents on ma ware scann ng gateways, endpo nt protect on and f rewa s.
Serv ces:	Bu d and/or test software for W ndows, nva d ty argument strategy, non- nfr ngement argument strategy, report preparat on, source code rev ews.

Str keforce, Inc. v. **Entrust et al.**

Case:	Case # 1:17-cv-00309
Descr pt on:	L t gat on re ated to patents on authent cat on techno og es.
Serv ces:	Inva d ty argument deve opment, non- nfr ngement argument deve opment, report draft ng.

Sony Corporation, Inc. v. Arr s

Case:	Inv. # 337-TA-1049
Descr pt on:	L t gat on re ated to patents on te ev s on stream ng dev ces and/or serv ces.
Serv ces:	Va d ty argument deve opment, source code rev ew of ent re p atform codebase nc ud ng numerous embedded p atforms, nfr ngement argument deve opment.

Kudelski SA, Nagra USA, Inc., Nagravision SA, and OpenTV, Inc. v. Comcast Corporat on

Case:	Case # 2:16-cv-1362-JRG, Inv. # 337-TA-1049
Descr pt on:	L t gat on re ated to patents on te ev s on stream ng dev ces and/or serv ces.
Serv ces:	Va d ty argument deve opment, source code rev ew of ent re p atform codebase nc ud ng numerous embedded p atforms, nfr ngement argument deve opment.

Amazon.com Inc., Hulu, LLC, and Netflix, Inc. v. Un oc Luxembourg S.A.

Case:	IPR 2017-00948
Descr pt on:	L t gat on re ated to patents on DRM protect on for content d str but on
Serv ces:	Pr or art search, PGR Preparat on, IPR preparat on.

Ph shMe v. **Wombat Technologies, Inc.**

Case:	Case # 16-403-LPS-CJB
Descr pt on:	L t gat on re ated to patents on ant -ph sh ng tra n ng techno og es.
Serv ces:	Pr or art search, PGR Preparat on, IPR preparat on.

Nader Asghar -Kamran and Kamran Asghar -Kamran v. **United States Automobile Association**

harborlabs
CYBER. SCIENCE

Case:	Case # 2:15-cv-478
Descr pt on:	L t gat on re ated to patents on authent cat on techno og es.
Serv ces:	Pr or art search, nva d ty argument strategy, non- nfr ngement argument strategy, source code rev ews

V r2us v. **Invincea Inc. and Invincea Labs, LLC**

Case:	Case # Case 2:15-cv-00162-HCM-LRL
Descr pt on:	L t gat on re ated to patents on v rtua zat on and automated corrupt on repa r.
Serv ces:	Pr or art search, nva d ty argument strategy, non- nfr ngement argument strategy, source code rev ews

Palo Alto Networks v. F njan

Case:	IPR 2016-00159, IPR 2016-00151, IPR 2015-01974, IPR 2015-02001, IPR 2015-01979
Descr pt on:	L t gat on re ated to patents on ma ware scann ng gateways and f rewa s,
Serv ces:	Pr or art search, patent nterpretat on, IPR preparat on support, c a m chart rev ew

TVIIM v. **McAfee**

Case:	Case # 3:13-cv-04545-VC
Descr pt on:	L t gat on re ated to patents on vu nerab ty scann ng
Serv ces:	Bu d and test software for SPARC/L nux/W ndows, patch out cense checks/crack software (w th perm ss on), obta n hard-to-f nd egacy software, pr or art and non-nfr ngement argument strategy support, source code rev ews, pr or art search

Al Cioffi et al. v. Goog e

Case:	Case # 2:13-cv-103-JRG-RSP
Descr pt on:	L t gat on re ated to patents on browser sandbox ng and process so at on.
Serv ces:	Code rev ew/software test ng to co ect ev dence of nfr ngement, Infr ngement argument preparat on support, c a m chart rev ew

Rovi Solutions & Veracode v. Appthor ty

Case:	Case # 12-10487-DPW
Descr pt on:	L t gat on re ated to patents on stat c debugg ng too s
Serv ces:	Source code rev ew refut ng oppos ng expert test mony

Pre-Harbor Labs Security Design and Software Development Experience

2013 At *Applied Communication Sciences*

Ro e:	Graduate Intern
Techno og es:	JavaScr pt, Python, Tcpdump, W reshark

- Deve oped extens b e rea -t me traff c v sua zat on too to chart and ana yze h gh-vo ume tcpdump streams of ossy metropo tan-area mesh network traff c.

2011 At *University of Michigan ICPSR*

Ro e:	Penetrat on Tester
Techno og es:	Numerous Secur ty Too s, Amazon EC2, VMware VSphere

- Conducted w de-sca e penetrat on test ng on v rtua zed c oud-based systems meant to be secure

harborlabs
CYBER. SCIENCE

env ronments for researchers to store conf dent a resu ts
- Created forma threat mode document deta ng potent a secur ty vu nerab t es from a poss b e attack vectors
- Wrote two reports deta ng resu ts from penetrat on test

2009-2011 At *Independent Security Evaluators*
Ro e: Secur ty Intern
Techno og es: C++, C#, Da v k Bytecode, Gcov, GDB, Javascr pt, Peach Fuzzer, Python, RegEx, XML, W reshark

- Created og pars ng framework to ana yze 20+ og f e formats
- Ass sted w th ma ware test ng, research and ana ys s
- Reverse eng neered DRM schemes n Andro d and IOS app cat ons
- Researched and prototyped secure cryptograph c ma de very system
- Deve oped web craw er to co ect f e sets for use n fuzz ng
- Wrote code-coverage ana ys s too for construct ng m n mum f e set for fuzz test ng
- Wrote fuzz ng p ug ns us ng Peach Fuzzer framework and reverse eng neered b nary f e spec f cat ons
- Wrote Internet Exp orer and Chrome extens ons for cryptograph c proxy system
- Created and debugged network protoco s for use n network protoco test ng
- Wrote and debugged un t tests n C++ and Python for propr etary d sk-encrypt on system

2008-2010 At *Johns Hopkins University DRCC*
Ro e: Student Programmer
Techno og es: DOM, Java EE, JSP Per , SAX, XSLT

- Drafted a report deta ng secur ty recommendat ons for an NSF funded data conservancy project
- Set up and dep oyed a Fedora d g ta repos tory w th the Is andora frontend
- Ported IRStats stat st cs package to the DSpace nformat on repos tory XMLUI
- Wrote batch mporter that s now used to mport more than 20 d g t zed books a week nto DSPace repos tory

2008 At *Brandeis University Information Technology Services Hardware Repair Shop*
Ro e: Free ance Programm ng Consu tant
Techno og es: Java, V sua C++, VBScr pt

- So e programmer on project to nterface Request Tracker t cket ng system w th Brother PT- 9500PC Labe Pr nter

Technical Skills

Languages	BASH, C, C++, C#, HTML, Java, JavaScr pt, Object ve-C, MATLAB, Python, Per , PHP, Regu ar Express ons, SQL, XML
Architectures	6502, 8051, 8080, ARM Cortex-M, ARMv7, ARMv8, AVR, m68k, MIPS, MSP430, PIC, SPARC, PowerPC, x86, x86-64, Z80
Operating Systems	Andro d, ChromeOS, FreeBSD, OS, OpenBSD, L nux, macOS, W ndows
DevOps and Development Tools	Ans b e, Ant, B tBucket, Conf uence, Docker, gdb, g t, G tHub, G tLab, Grad e, Hadoop, jad, jd-gu , J ra, Maven, make, MySQL, PostgreSQL, subvers on, Tre o, Vagrant, va gr nd
Security Tools	A rcrack-ng, apktoo , b nwa k, bu k-extractor, Burp su te, Char es Proxy, cur , dex2jar, ftk, hashcat, IDA Pro,

harborlabs
CYBER.SCIENCE

Cloud and Virtualization	Metasp o t, m tmproxy, Nessus, nmap, OpenSSL, ophcrack, p0f, Sca pe , sk pf sh, snort, ss str p, ss yze, Vo at ty, Web Scarab, wget, W reshark AWS, Azure, Bhyve, KVM, LXD, QEMU, v rt-manager, VMware, Xhyve

Honors, Societies and Awards

- Member Ups on P Eps on Internat ona Computer Sc ence Honor Soc ety
- Member Inst tute for E ectr ca and E ectron cs Eng neers (#97507890)
- Member Assoc at on for Comput ng Mach nery (#9700346)

At Johns Hopkins University

- Computer Sc ence Department Outstand ng Teach ng Ass stant Award
- Treasurer, Ups on P Eps on Internat ona Computer Sc ence Honor Soc ety (JHU Chapter)
- Computer Sc ence Department Facu ty L a son Czar
- Student Representat ve to the Computer Sc ence Undergraduate P ann ng Curr cu um Comm ttee

Attachment B

Materials Considered

Case Documents

Pleadings

- Complaint, *Surgical Instrument Service Co., Inc. v. Intuitive Surgical, Inc.*, No. 3:21-cv-03496-VC (ECF 1) (May 10, 2021)
- Consolidated Amended Class Action Complaint, *In re: da Vinci Surgical Robot Antitrust Litigation*, Lead Case No. 3:21-cv-03825-VC (ECF 52) (Sept. 9, 2021)

Expert Reports

- Expert Report of Christy Foreman (Jan. 18, 2023)
- Expert Report of Kurt Humphrey (May 10, 2021)
- Expert Report of Kurt Humphrey, submitted in the matter of *Rebotix Repair LLC v. Intuitive Surgical, Inc.*, Case No. 8:20-cv-02274 (M.D. Fla.) and dated July 26, 2021

Deposition Transcripts and Exhibits

- Deposition of Grant Duque 30(b)(6) (November 8, 2022)
- Deposition of Grant Duque (November 8, 2022)
- Deposition of Sharathchandra "Shark" Somayaji (November 4, 2022)
- Deposition of Margaret Nixon (October 7, 2022)

Produced Documents

- Intuitive-00002201 - da Vinci Si Surgical System User Manual
- Intuitive-00002502 - da Vinci Xi System User Manual
- Intuitive-00499468
- Intuitive-00506505
- Intuitive-00538994
- Intuitive-00544903
- Intuitive-00861667
- Intuitive-00994614
- Intuitive-00999731 (Somayaji Deposition, Ex. 224) - Atmel CryptoRF EEPROM Memory Summary Datasheet
- Intuitive-01004232
- Intuitive-01004242
- Intuitive-01004385

Other Documents

- Annalee Newitz, *The RFID Hacking Underground*, WIRED, (May 1, 2006), available at: https://www.wired.com/2006/05/rfid-2/.
- Atmel CryptoRF EEPROM Data Sheet.
- Dale Anderson, *Understanding Crypto Memory the World's Only Secure Serial EEPROM*, ATMEL (2004).
- Dallas Semiconductor DS2505 Data Sheet.
- GITHUB, *Proxmark3*, available at: https://github.com/Proxmark/proxmark3 (last visited Jan. 18, 2023).
- Grassi et. al., *Digital Identity Guidelines*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, June 2017, available at: https://doi.org/10.6028/NIST.SP.800-63-3.
- KASPERSKY, *What is Spoofing - Definition and Explanation*, available at: https://www.kaspersky.com/resource-center/definitions/spoofing (last accessed Jan. 18, 2023).
- Martin et. al., *Applications of Secure Location Sensing in Healthcare*, Proceedings of the 7th ACM International Conference on Bioinformatics, Computational Biology, and Health Informatics (2016).
- OPENSSH, available at: https://www.openssh.com/ (last visited Jan. 18, 2023).
- Products Specifications, INTEL, available at: https://ark.intel.com/content/www/us/en/ark/search/featurefilter.html?productType=873&1_Filter-SocketsSupported=3562 (last visited Jan. 18, 2023).
- RFID Readers, AMAZON, available at https://www.amazon.com/RFID-Readers/s?k=RFID+Readers (last visited Jan. 18, 2023).
- Tyler Petersen, *RFID Card Security and Attacks*, (Oct. 15, 2020), SIKITCH, available at: https://www.sikich.com/insight/rfid-card-security-attacks-and-prevention/#:~:text=An%20MITM%20attack%20against%20an,gain%20access%20to%20the%20building.